



# Cyber Security Engineering and Research @ JPL

**Dr. Arun Viswanathan**

Cyber Defense Engineering and Research Group



**Jet Propulsion Laboratory**  
California Institute of Technology

# About Me

## M.S., Ph.D. in Computer Science (Cybersecurity)

Dec 2015

University of Southern California

Advisor: Dr. Clifford Neuman

## Cybersecurity researcher @ JPL

Apr 2015 - *present*

Cyber Defense Engineering and Research (CDER) Group

- Task lead on a project to improve cyber situational awareness of JPL missions
- Applied cyber security research

## Research interests

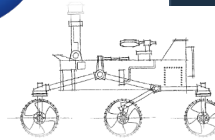
- Cyber situational awareness
- Secure Autonomous Systems
- AI/ML techniques for cybersecurity
- Robust detection methods
- Model-based Reasoning and Analysis
- Detection, diagnosis and response

# Cyber Defense Engineering and Research (CDER) Group

13+ members, 3 PhD's, Diverse Backgrounds

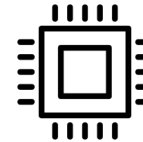
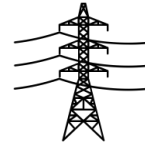
## Project/Program Office Cyber Defense Engineering

- Supports *Cyber Security Improvement Project*



## Technology development / Fundamental research in Cyber Security

- JPL funded research
- Non-NASA Reimbursable tasks (Power Grid, Oil and Gas, DoD, NSF, DARPA)



"Oil Derrick" by Nikita Kozin, from [thenounproject.com](http://thenounproject.com)

"Transmission Tower" by Arthur Shlain, from [thenounproject.com](http://thenounproject.com)

"Processor" by Creative Stall, from [thenounproject.com](http://thenounproject.com)

# Cyber Security Research Areas in CDER

## Model-based Approaches for Cyber Security

- Model-based risk assessment
- Model-based diagnostics for correlation and root cause analysis
- Automated attack-tree generation

## Security of Autonomous Systems

- Automated assessment of cyber-risks to autonomous vehicles.
- Cyber-physical resilience of autonomous systems.

## Mission-centric Cyber Situational Awareness

- Advanced data analytics
- Correlation and diagnostics
- Advanced UI/UX
- AI-based alerting

## Robust Detection

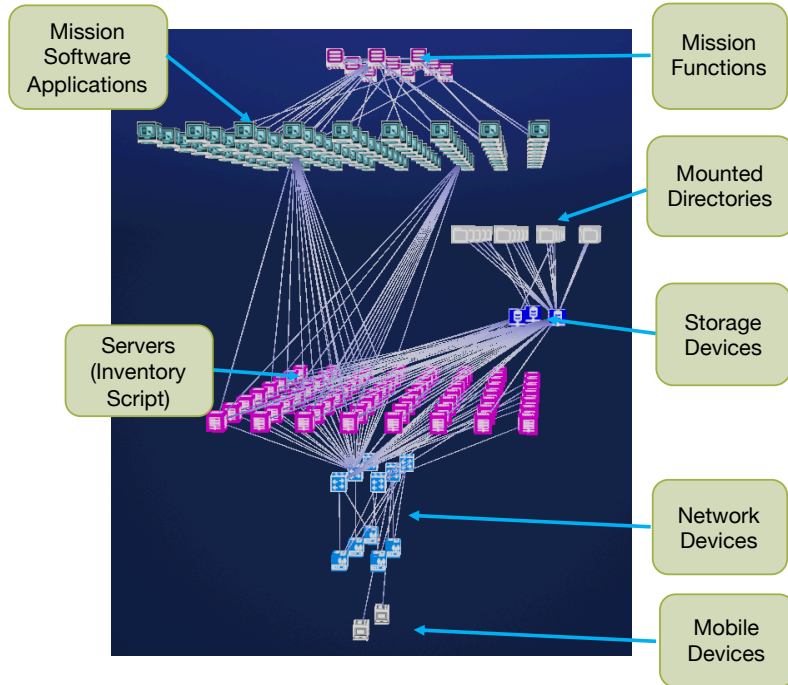
- Anomaly detection in mission critical environments with low error tolerance
- Advanced ML-based techniques for detecting cyber intrusions
- Explainable machine learning

## Hardware/Embedded Cyber Security

- Anti-Tamper technologies for embedded and reconfigurable devices
- Resilience of encryption engines
- Firmware reverse engineering
- Side-channel analysis including functional, EMC/EMI, RF for embedded devices

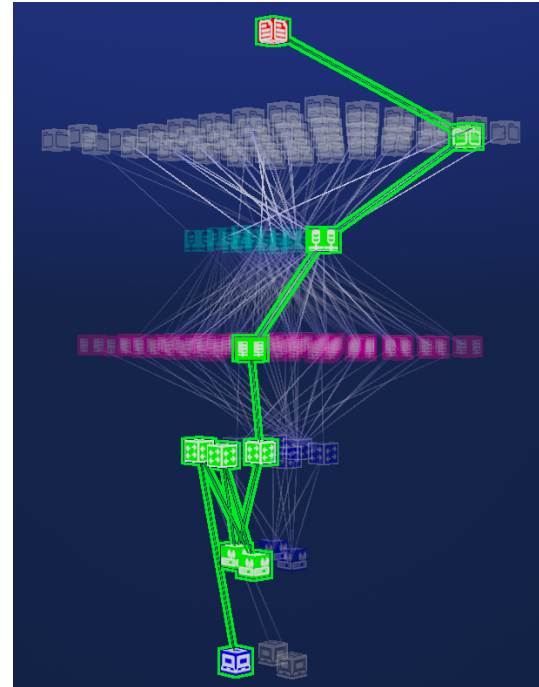
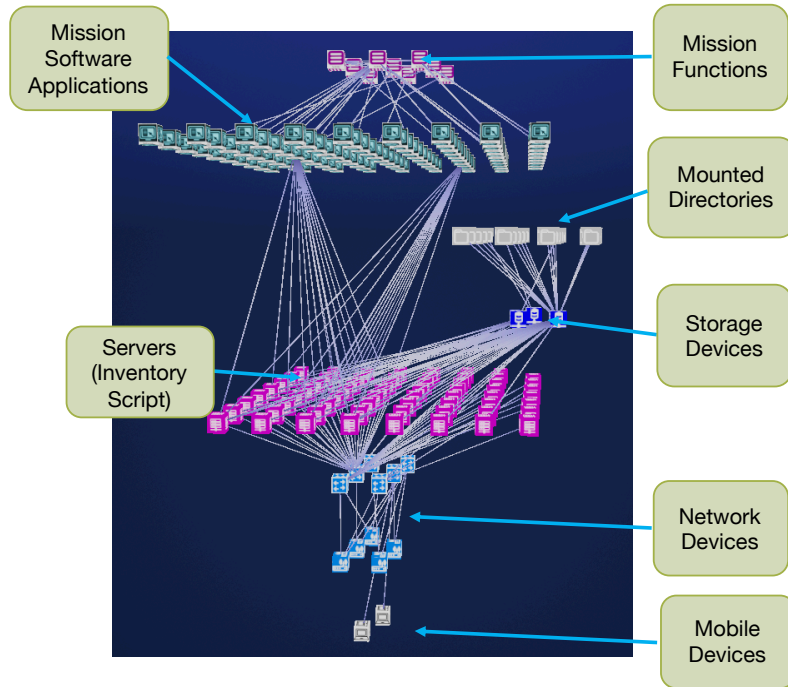
# Cyber Analysis and Visualization Environment (CAVE)

## Model-based approaches for cybersecurity



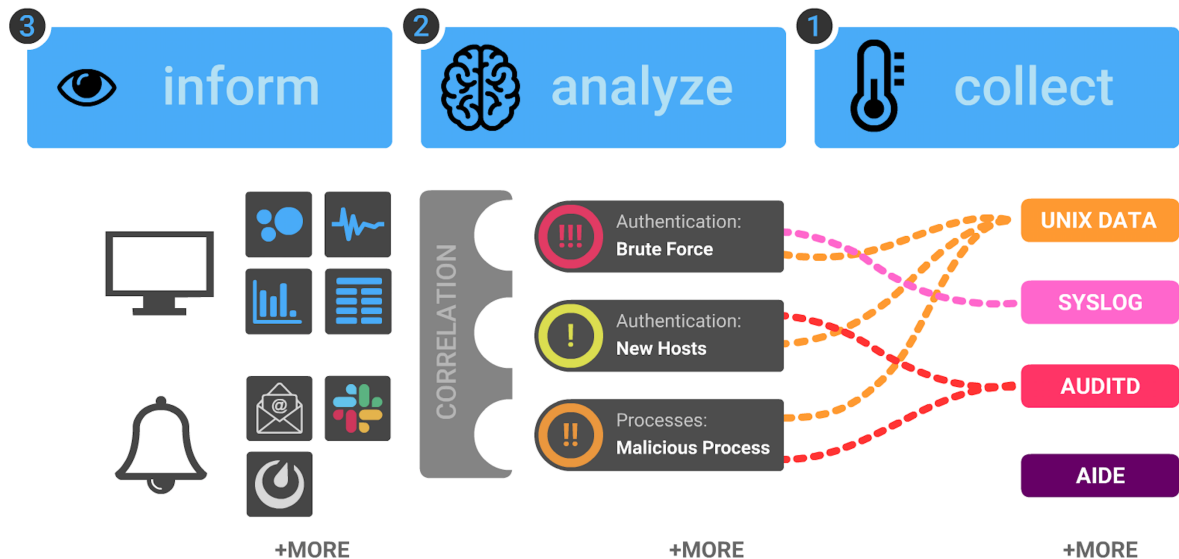
- JPL-developed, extensible, software framework to be used by cyber analysts.
- Multi-layered cyber-physical system model
  - Hardware, software, files, processes, network connections, vulnerabilities , cost, risk
- Model-based reasoning
  - Determine consequences of adversarial activities to mission objectives
  - Report cyber-physical inventory to the mission
  - Track possible adversary entry/paths/goals given known weaknesses in our mission environment (i.e. CVEs, node centrality, proximity to the internet )
- Currently modeling missions in flight and development

# Example Reasoning in CAVE



# Cyber Situational Awareness for Missions (CyberSAM)

## Mission-centric Cyber Situational Awareness



**Objective** Improve situational awareness of mission engineers, assisting them to

- ✓ **detect, diagnose** and **respond** to cyber attacks; and
- ✓ identify anomalous system behaviors.

Currently deployed in service of 10 JPL missions,

MRO, M2020, NISAR,  
Psyche, DSN, Europa  
Clipper, Juno, SWOT,  
Sentinel-6, Lunar Flashlight

# Cyber Defense Laboratory

- Project Cyber Validation & Verification
  - Project-specific verification of vulnerabilities, mitigation design, mitigation validation.
- Project Systems Simulation and Emulation
  - Ground systems.
  - Flight systems.
  - Communications.
  - Support infrastructure services within an isolated environment.
- Cyber-focused Research to support Missions
  - Modeling, analysis, detection, diagnosis, remediation.
  - GPU-hardware for advanced machine learning-based research



# Research: Robust Anomaly Detection

## Challenges In Operational Mission Critical Environments

Current anomaly detection products are not deployable in mission environments

- Imprecise measures of capability, e.g., poor metrics
- Not built with mission requirements, e.g., adaptability to mission phasing, dial-up/down of resources
- Poor knowledge and characterization of performance
  - No concept of failure profiles in evolving environments (threat and infrastructure)
  - No science behind the study of errors, e.g., when do errors occur and how can we compensate for them?
- Many black boxes with no understanding of when and how performance changes cascade to affect down-stream decision-making processes
- Many claims with little evidentiary support (independent validation)

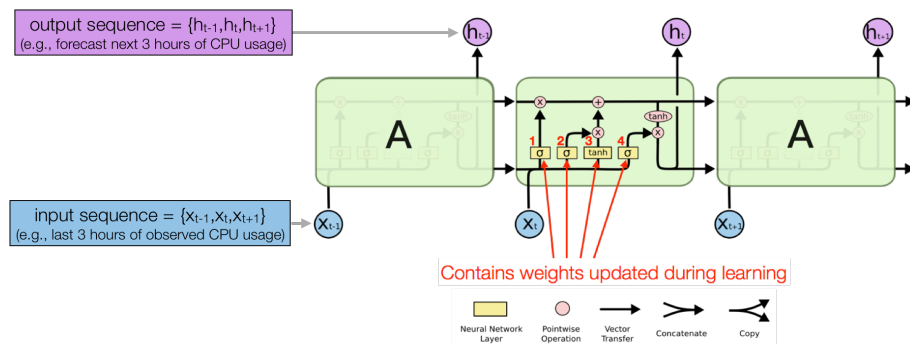
# Research: Robust Anomaly Detection with LSTMs

## Collaborative Research with Machine Learning Group at JPL

**Objective:** Develop a robust anomaly detector for detecting anomalies in ground data systems, using system health data metrics.

**Approach:** LSTM neural network capable of identifying subtle changes in system health data streams while also modeling both long and short term temporal behavior

**Key Step:** Rigorously evaluate the LSTM within mission environments, explain the LSTM performance in detail (*what is it good at?, where does it fail?*)



LSTM Neural Network Architecture for Detection

# Security and Resilience of Autonomous Systems

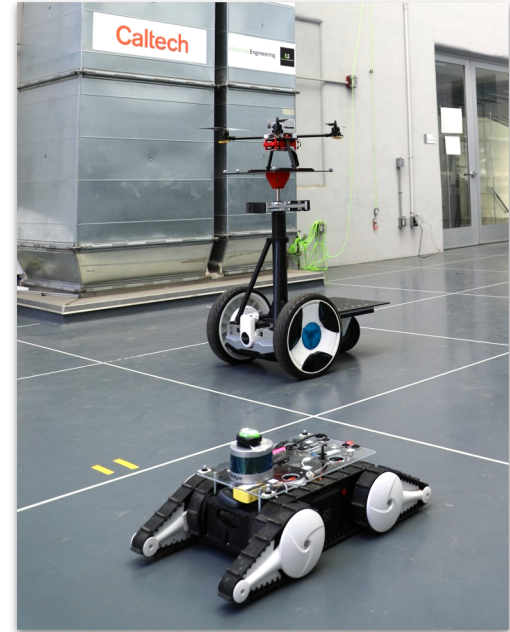
## New projects proposed for FY20

Automated assessment of cyber-risks to autonomous vehicles (with Stanford)

*Objective* Develop a methodology to enable assessment of cyber vulnerabilities as well as to recommend risk reduction method.

Cyber-physical resilience of autonomous systems (with Caltech)

*Objective* Demonstrate how a team of autonomous agents with heterogeneous capabilities can cooperate to achieve a goal, even in the presence of adversarial activity.



Picture courtesy: Caltech Center for Autonomous Systems and Technologies (CAST)



**Jet Propulsion Laboratory**  
California Institute of Technology

---

[jpl.nasa.gov](https://jpl.nasa.gov)